In the United States Patent and Trademark Office

028420-0013CON

In re Application of:	
Inventor(s):	Paul C. Kocher, Joshua M. Jaffe, Benjamin C. Jun
Serial No.:	Not Yet Assigned
Filing Date:	August 15, 2001
Title:	Cryptographic Computation Using Masking to Prevent Differential Power Analysis and Other Attacks
which is a continuation of application:	
Serial No.:	09/324,798
Filing Date:	June 3, 1999
Title:	DES and Other Cryptographic Processes with Leak Minimization for Smartcards and Other Cryptosystems

Art Unit: 2132

Examiner: J. Darrow

Certificate of Mailing Under 37 C.F.R. 1.10

Pursuant to 37 C.F.R. 1.10, I hereby certify that this paper and all enclosures are being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" (Label No. EL 728 498 770 US) on the date indicated below in an envelope addressed to the Commissioner for Patents, Washington, D.C. 20231.

Date: August 15, 2001

Name of Person Mailing: Jan Steele

Jan Steele

Signature of Person Mailing

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

Before considering the above-identified application on its merits, please amend the application as follows:

**** Remainder of Page Is Intentionally Left Blank ****

AMENDMENT TO SPECIFICATION

1. Please substitute the following amended title for the pending title on page 2, beginning on line 1 and ending on line 2, as follows:

--CRYPTOGRAPHIC COMPUTATION USING MASKING TO PREVENT DIFFERENTIAL POWER ANALYSIS AND OTHER ATTACKS—

2. Please substitute the following amended paragraph for the pending two paragraphs on page 2, beginning on line 4 and ending on line 7, as follows:

--This application is a continuation of U.S. Application No. 09/324,798, filed June 3, 1999 (which is hereby incorporated by reference in its entirety), which claims the benefit of U.S. Provisional Application No. 60/087,826, filed June 3, 1998. U.S. Application No. 09/324,798 is related to co-pending U.S. Application No. 09/224,682, filed December 31, 1998.--

**** Remainder of Page Is Intentionally Left Blank ****

VERSION OF AMENDED SPECIFICATION WITH MARKINGS TO SHOW CHANGES MADE

1. The title on page 2, beginning on line 1 and ending on line 2, has been amended as follows:

[IMPROVED DES AND OTHER] CRYPTOGRAPHIC [PROCESSES WITH LEAK MINIMIZATION FOR SMARTCARDS AND OTHER CRYPTOSYSTEMS] COMPUTATION USING MASKING TO PREVENT DIFFERENTIAL POWER ANALYSIS AND OTHER ATTACKS

2. The paragraphs on page 2, beginning on line 4 and ending on line 7, have been amended as follows:

This application is a continuation of U.S. Application No. 09/324,798, filed June 3, 1999 (which is hereby incorporated by reference in its entirety), which claims the benefit of U.S. [provisional patent application no.] Provisional Application No. 60/087,826, filed [on] June 3, 1998. [This application] U.S. Application No. 09/324,798 is related to co-pending U.S. [patent application no.] Application No. 09/224,682, filed [on] December 31, 1998.

**** Remainder of Page Is Intentionally Left Blank ****

AMENDMENT TO CLAIMS

Please cancel claims 1-40 without prejudice.

Please add the following new claims 41-50:

41. A method for performing a cryptographic operation with resistance to external monitoring attacks, where said cryptographic operation includes performing a substitution operation using a predefined substitution table, said method comprising:

(a) obtaining a representation of a predefined substitution table specifying a corresponding table value for each of a plurality of possible table index values;

(b) using random information, transforming said representation of said predefined substitution table into a new randomized representation of said substitution table;

(c) receiving a datum to be cryptographically processed;

(d) computing a blinded representation of a table index value from at least said datum;

(e) using said new randomized representation of said table, performing a substitution on said blinded table index value to derive a blinded representation of the table value corresponding to an unblinded version of said table index value in step (d); and

(f) using said blinded table value to compute a cryptographic result for use in securing a cryptographic protocol.

42. The method of claim 41, where said step (d) includes the substeps of:

(i) obtaining an input masking parameter; and

(ii) deriving said blinded table index value from at least said input masking parameter and said received datum.

43. The method of claim 42, where said blinded representation of said table value constitutes said unblinded version of said table value in step (e), exclusive-ORed with an output masking parameter whose value depends on said random information.

44. The method of claim 41, where said transforming in step (b) includes permuting a plurality of entries in said predefined substitution table.

45. The method of claim 41, where said transforming in step (b) includes computing at least one value in said randomized representation of said substitution table by exclusive-ORing at least one masking value with at least one value of said predetermined substitution table.

46. The method of claim 41, where said transforming in step (b) includes representing said predefined substitution table as a plurality of tables.

47. A method for performing a cryptographic operation involving a substitution operation using a predefined substitution table, comprising:

(a) obtaining random information;

(b) using said random information, producing a randomized representation of said table;

(c) receiving a datum to be cryptographically processed;

(d) applying said randomized representation of said table to a table input derived from at least said datum to produce a substitution result randomized by said random information;

(e) using said randomized substitution result, deriving a cryptographic result, where said cryptographic result is independent of said random information; and

(f) using said cryptographic result as part of securing a cryptographic protocol.

48. A device for performing a cryptographic operation, where said cryptographic operation involves a key and an input message and includes a substitution operation with a predefined substitution table, comprising:

(a) a source of random data;

(b) table randomization logic configured to use an output from said source of random data;

(c) a memory for storing a randomized representation of a predefined substitution table;

(d) table input parameter computation logic, configured to produce a table input parameter from at least a portion of an input message and said output from said source of random data;

(e) first cryptographic computation logic configured to perform substitution operations on said table input parameter using said randomized representation of said predefined substitution table in said memory;

(f) second cryptographic logic, configured to use said first cryptographic computation logic to compute a cryptographic result, where said cryptographic result depends solely on said key and said input message and is independent of said output from said source of random data.

49. The device of claim 48 where said source of random data is a pseudorandom number generator.

50. The device of claim 48 where said source of random data includes a source of truly random values.

VERSIONS OF AMENDED CLAIMS WITH MARKINGS TO SHOW CHANGES MADE

Claims 1-40 have been deleted.

New claims 41-50 have been added.

**** Remainder of Page Is Intentionally Left Blank ****

REMARKS

This application is a continuation of U.S. Application No. 09/324,798, filed June 3, 1999, which claims the benefit of U.S. Provisional Application No. 60/087,826, filed June 3, 1998. U.S. Application No. 09/324,798 is expected to issue as U.S. Patent No. 6,278,783 on August 21, 2001.

This continuation application cancels claims 1-40 and adds new claims 41-50. In addition, Applicants have amended the specification to add specific references to earlier applications. No new matter has been added.

CONCLUSION

Applicants respectfully request the entry of the foregoing amendment prior to examination of this continuation application. If the Examiner believes that the prosecution of the application can be expedited through a telephone interview, the Examiner is invited to call the Applicants' attorney, Joe Yang, at (650) 470-4565.

Respectfully submitted,

Date: August 15, 2001

Joseph Yang, Ph.D.
Registration No. 41, 387

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570